

# **Education in the 'Virtual' Community: Can beating Malware Man Teach Users about Social Networking Security?**

A. Sercombe and M. Papadaki

Centre for Security, Communications and Network Research  
Plymouth University, United Kingdom  
e-mail: [info@cscan.org](mailto:info@cscan.org)

## **Abstract**

Social Networks have become part of daily life for millions of people and by their very nature they encourage information sharing, which poses a significant security challenge. 2011 has seen numerous targeted "Spear Phishing" attacks in which the attackers have gained knowledge about victims before carrying out the attack. Social media has been utilised as the source for this information so therefore it is even more important that users are educated against the risks (Symantec, 2011).

This paper looks the current threats and awareness strategies. It describes the design and evaluation of an online game to help educate users. The game has a central 'Malware Man' character and a firewall which burns him if the player answers correctly. The success of the game was then evaluated using an experiment with a group of participants who had played the game, and a control group who had not. 101 users participated in the study. The results showed that the game was successful in educating users, as the average percentage of correct answers was 77% for those who had played the game, compared to 55% for those who had not.

## **Keywords**

Social Networking, Social Networks, Phishing, Spear Phishing, Education, Awareness, Game, Interactive

## **1 Introduction**

Social Networks are defined as 'networks of social interactions and personal relationships' (Oxford Dictionary, 2011). They are used to build online communities of people who share interests with one another (Shin, 2010). Facebook alone, reports that it has over 800 million active users, of which more than 50% logon every day (Facebook, 2012). This makes social network sites a very lucrative target for attackers. There is a large amount of data to mine and a plentiful supply of users that can be targeted.

These threats not only affect individuals, but also pose a risk to organisations and even governments and infrastructure. 2011 has seen a decrease in the amount of spam detected, but an increase in targeted attacks (Symantec, 2011). It is suggested

that attackers may be moving away from spam and choosing to use social networks to mine information so they can perform more targeted attacks.

In the last week a security company called Stratfor has been hacked and has released an announcement on Facebook stating that they have evidence that users or employees who have posted messages of support on the social networking site are being specifically targeted (BBC, 2011). This is further evidence that information on social media sites is being used by hackers as a standard information gathering tool, and can also be used to target individuals.

## **2 Social Networking Threats**

Before you can start to design a game to educate users you need to understand the threats. The following is a list of the main threats against social networks.

### **2.1 Spam**

Spam can be defined as 'unsolicited messages propagated through a medium' (Hogben, 2007 p11). It is one of the oldest, simplest and most common attacks and it is very quick to adapt to new technologies. Social networks are usually free to use and free to send messages, which mean that they are an ideal candidate for spammers.

### **2.2 Social Engineering**

One of the ways that social networks have been targeted is by the use of social engineering attacks. These attacks often take advantage of the fact that there is pressure on social networking users to have the most 'friends' or 'followers' (Symantec, 2010, p3). Phishing is a common type of social engineering attack and is used against social networks. In a study by Jagatic, Johnson, Jakobson and Menczer (2007), they used freely accessible social networking information to create crafted emails that appeared to be from friends of the victim, and they found that the targets were much more likely to give away information to a friend than to a stranger.

### **2.3 Trojans/Malware**

The W32 Koobface worm was one of the first large scale malware attacks targeting social networks and is said to still be active today. It is very successful and relies on social networking users link opening behaviours. (Symantec, 2010, p3).

### **2.4 Applications**

Some social networks allow active content to be embedded in pages. Examples of applications include daily horoscopes and quizzes. Some social networks allow remote code to be included, but most larger networks use APIs to restrict the access that these applications have.

## **2.5 Content threats**

There are various content threats that have been used against social networking users. Some of the most serious include utilising vulnerabilities in the underlying software to embed malicious content inside profiles. One of the easiest ways to perform an attack is to use malicious links. URL shortening makes it hard for even savvy users to check if a request is genuine.

## **2.6 Privacy**

Privacy is a serious concern for social networking users. It is important that the user has control and can easily restrict information. Once a message is posted, it is almost impossible to delete it because of the nature of internet caching. Information disclosure such as location data and private information is also a concern. (West 2010, p26).

## **3 Awareness Strategies**

There are a number of different strategies used to raise awareness about security threats, and there has been considerable research in this area. The U.K. government, law enforcement and a number large organisations sponsor a Get Safe Online initiative ([www.getsafeonline.org](http://www.getsafeonline.org)) (Furnell, Bryant & Phippen, 2007). The web site offers videos, guides, reports and help for users and small businesses to raise their security awareness.

Globally there are numerous initiatives, for example the European Network and Information Security Agency (ENISA) have an awareness raising program which consists of workshops, conferences, literature.

## **4 Malware Man Design**

A number of requirements were collated as a result of learning and education research and literature review. The key requirements are listed below:

### **4.1 Non-functional Requirements**

- Captivate player attention (Dondlinger, 2007)
- The game design must promote and foster learning (Dondlinger, 2007)
- Use design elements from video games to encourage game play (Dondlinger, 2007)
- Narrative context is key to making the game engaging and fun (Sheng et al., 2007)
- A strong character and story will help motivate players. (Sheng et al., 2007)
- An emphasis on skill as there must be a challenge to prevent players getting bored

- Stimulate desired learning outcomes using goals and rewards (Dondlinger, 2007)

## 4.2 Functional Requirements

- The game should be dynamic and easily configurable for different types of Social Networks. The game will be more relevant to users if it can be customized.
- Platform independence. It is important that the game is available to as wide a group of users as possible.

## 4.3 Design

The game was developed using Adobe Flash Builder 4.5 using the flex development language which builds a .swf file. This ensures that the game will run on any browser as long as it has Flash Player 10 or above installed.

There are three game states; 'Start', 'InGame' and 'End'. If the user answers correctly, a flickering animated firewall increases in size and a speech bubble appears giving the impression that Malware Man is being hurt.

Help information appears providing the user more information about the question and the correct answer after they have submitted their answer. If the user answers correctly then the text will be coloured green.



If the user answers incorrectly then the firewall stays the same size, and the wrong answer and hint text are coloured red. The right answer is coloured green, so that the user can immediately see where they went wrong.

The design of the questions in the game was centred around the main threats outlined earlier in this paper. The questions were all multiple choice based with four possible answers. Some questions used images from social networks, for example a wall posting from a Facebook feed to make the question more relevant to the user. Three sets of ten questions were created for three different versions of the game.

## **5 Evaluation Design**

The game needed to be evaluated to assess how successful it was in educating users. This assessment was done by carrying out a user study. The study consisted of one group of users who had played the game, and a control group who had not. Both groups were given the same survey to complete and the hypothesis was that the users that had played the game would answer more questions correctly.

There was also an informal feedback field in the survey for participants to give some qualitative feedback on the game.

The two sample groups included Plymouth University Masters and Undergraduate students and Met Office employees in the Technology and Information services department. All participants were over 18 years old and the study did not include vulnerable adults. An invitation email and a consent page outlined the aims of the research, contact details, a clear description of the right to withdraw at anytime and a reinforcement that participation is voluntary.

## **6 Results**

104 participants took part in the study, of which three results had to be discarded due to the fact that all the answers were blank. The overall percentages are 32% female, 65% male and 3% undisclosed. 51% of participants were aged between 26-35 and 32% were between 36-45. The other 17% were either 18-25, 46-55 or 56-65.

The results indicated that the percentage of correct answers for those users who played the game was 77% as opposed to 55% for those who did not. These results relate to the first 8 questions in the survey as these were the same for all users. The other questions were Facebook or Twitter specific and only appeared if users played those specific versions of the game but also gave very similar results.

It was also found that users did not do as well on the number based statics questions compared to those that were more descriptive. This is interesting as it suggests that the participants may learn better when the question answers are more descriptive in nature.

The informal feedback on the game showed that participants found the game to be generally good and informative, but there were some concerns over the clarity of the colours for users who may suffer from colour blindness. One participant suggested that a leader board may have added to the experience so they could see how they performed compared to other users.

## **7 Conclusions and Future Work**

This paper has given an overview of the current social networking threats and awareness campaigns and has then presented the design and evaluation of the Malware Game.

The results suggest that the game was successful in educating users as there was a large difference between the number of correct answers for those that had played the game compared to those who had not. The sample size was not sufficient to be conclusive and the participants belonged to quite a specific demographic.

Future research could include looking at different cultures and demographics of users, as well as using a larger sample size. It could also include extensions to the game for different levels and could give forms of reward to see if this improves the user experience.

Trialing the game against other forms of online educational material and carrying out a study to determine how well the game performed comparatively would give a better understanding of how effective the game is in educating users in comparison to other techniques.

## 8 References

BBC, 27/11/2011, 'Anonymous' hack victims face repeat attacks, BBC. Available from: <<http://www.bbc.co.uk/news/technology-16338680>>. [27/12/2011].

Dondlinger, MJ 2007, 'Educational video game design: A review of the literature', *Journal of Applied Educational Technology*, vol. 4, no. 1, pp. 21-31.

Facebook, Statistics - Facebook, Facebook. Available from: <<https://www.facebook.com/press/info.php?statistics>>. [05/01/2011].

Furnell, SM, Bryant, P & Phippen, AD 2007, 'Assessing the security perceptions of personal Internet users', *Computers & Security*, vol. 26, no. 5, pp. 410-417.

Hogben, G 2007, 'Security issues and recommendations for online social networks', *Position Paper ENISA European Network and Information Security Agency*, vol. 80211, no. 1.

Jagatic, TN, Johnson, NA, Jakobsson, M & Menczer, F 2007, 'Social phishing', *Communications of the ACM*, vol. 50, no. 10, pp. 94-100.

OxfordDictionary 2011, *Oxford Dictionaries - Definition of Social Network in Oxford Dictionaries*, Oxford University Press, [01/06/2011].

Sheng, S, Magnien, B, Kumaraguru, P, Acquisti, A, Cranor, LF, Hong, J & Nunge, E 2007, 'Anti-Phishing Phil: the design and evaluation of a game that teaches people not to fall for phish', in, *ACM*, pp. 88-99.

Shin, D-H 2010, 'The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption', *Interacting with Computers*, vol. 22, no. 5, pp. 428-438.

Symantec, CW- 2010, 'The Risks of Social Networking', *Symantec - Security Response*[12/05/2011].

Symantec, PW- 2011, *Symantec Intelligence Report: November 2011*, Symantec, [20/12/2011].